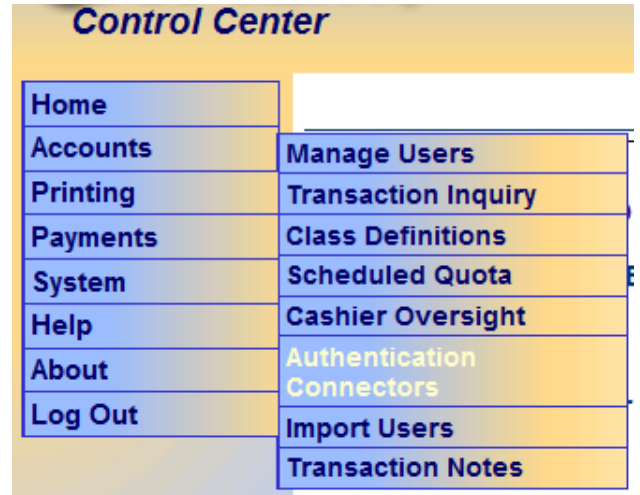




Novell OpenLDAP Configuration

To access the GoPrint Novell e-Directory LDAP Connector configuration screen navigate to:

Accounts – Authentication Connectors






GoPrint provides two connector options, Standard Authentication and Card Swipe Authentication. The card swipe authentication is used when the students Login Id is programmed on a university campus card and is used to release print jobs when swiped at a Print Release Station.

Step 1 - Click Add a Standard Authentication Connector


Authentication Connectors

Authentication connectors are listed below. You may add, edit, or reorder the items in the list. When a user authenticates the active authentication connectors will be attempted in the order listed here, until the user authenticates successfully with one of them or fails to authenticate with all of

Standard Authentication

Name	Type	Active
 Students	LDAP	Active
 Add a Standard Authentication Connector		
 Test Standard Authentication Connectors		

Card Swipe Authentication

Name	Type	Active
No Card Swipe Authentication Connectors have been defined.		
 Add a Card Swipe Authentication Connector		

Step 2 - Select Novell eDirectory



Step 3 – Enter the Connector

Name: create a unique user-friendly name to identify the connection type.

Active: click Active

LDAP Authentication - Step 1 of 3

Configure user authentication by searching and authenticating network logon IDs against LDAP

Connector

Enter a unique name for this connector.

Name

Active

Step 4 - LDAP ServerName and Security

ServerName: enter the OpenLDAP servers hostname

LDAP Server

Enter the LDAP server's network name.

ServerName

Security

Simple (no network privacy) ▼

Authentication Type: leave default of Simple (No network privacy) To enable SSL authentication the OpenLDAP schema must be enabled to force secure TLS communication, and the eDirectory SSL certificate must be imported into the Java cacerts keystore. Refer to "Advance Topics" under the GoPrint HELP section.



Step 5 - Enter the Base DN

Set to where you want the Search to start:

Example: Root level

Search Target

Set the Base DN that is the top-level target for searches.

Base DN

o=ccp

Example: Organization level or Container

Base DN

cn=users,dc=fandm,dc=edu

Browse



Save



Delete

Search User DN

OpenLDAP requires an authenticated user with Read permission to perform searching.

CN

Example 1: **cn=ldaproxy**

Search User Account

Enter the DN of a user account to use when searching the LDAP repository. Most LDAP servers require an authenticated user to perform searching, and one is recommended even if not required. If left blank, an 'anonymous bind' will be used to search.

Search User DN

cn=ldaproxy



Append Base DN

Password

Previously Set



Test connectivity when Next is pressed

UID

Example 2: **uid=goprintldap**

Some LDAP servers require an authenticated user to perform searching. If yours does, enter a user account that can be used below. If left blank, an 'anonymous bind' will be used to search.

Search User DN

uid=goprintldap



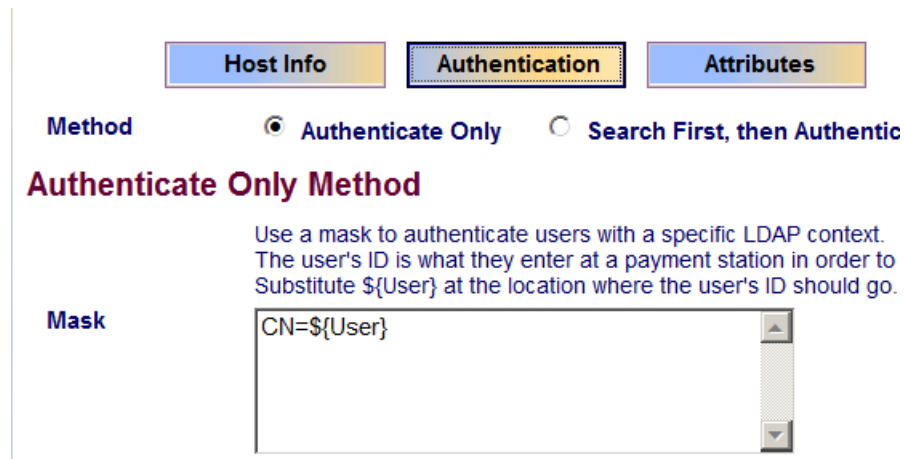
Append Base DN

Password

Previously Set

Step 6 – Search First, then Authentication

The default authentication mask of CN=\${User} is usually sufficient.



Host Info **Authentication** **Attributes**

Method **Authenticate Only** **Search First, then Authentic**

Authenticate Only Method

Use a mask to authenticate users with a specific LDAP context. The user's ID is what they enter at a payment station in order to Substitute \${User} at the location where the user's ID should go.

Mask

Other Mask Options

Your campus may be using specific filters, such as eduPersonAffiliation

(&(uid=\${User}))(eduPersonAffiliation=Student))

Method **Authenticate Only** **Search First, then Authenticate**

Search and Authenticate Method

Use an LDAP search filter to perform a search in order to locate the user account to authenticate with, then a subsequent authentication to verify their password. Substitute \${User} in the filter to indicate where the user's ID should go. The user's ID is what they enter at a PayPoint in order to pay for their print jobs.

Search Filter



Step 7 - Attributes

Account ID: use cn or uid

Class Name: optional

Default Class: Select User Class users will be assigned

Card Number: optional. Used with 3rd party transaction systems

FirstName: name

LastName: sn

Reference Number: optional

E-Mail: Optional

Attributes

Enter the LDAP attribute names that your system CN or sAMAccountName, but can equally be an user identifier.

Account ID	<input type="text" value="uid or cn"/>
Class Name	<input type="text"/>
Default Class	<input type="text" value="Staff"/>
Card Number	<input type="text"/>
First Name	<input type="text" value="name"/>
Last Name	<input type="text" value="sn"/>
Reference Number	<input type="text"/>
E-Mail	<input type="text" value="mail"/>
<input type="button" value="Attribute Browser"/>	

Step 8 – Test the LDAP Connection

You can run a connection test using the connector Test utility to ensure your LDAP settings are correct.

Click the Test button

Host Info Authentication

Connector

Name

Active

Host Info



Authentication Test

Enter a username and password located in the search filter path

Click: Test

Authentication Test

Here you may test an authentication profile setting. Select which authentication profile to test and enter a username/password to test with.

Authentication Profile	Active Profiles
Username	<input type="text"/>
Password	<input type="password"/>
	<input type="button" value="Test"/>

A successful query returns the following results:

Test Result	Successful				
	NOTE: This is only a test. An account has not been created.				
Using Connector	Students				
Connector Type	LDAP				
User ID	steve				
First Name	steve				
Memberships	<table border="1"><thead><tr><th>Class Name</th><th>Class Type</th></tr></thead><tbody><tr><td>Default User Class</td><td>USERS</td></tr></tbody></table>	Class Name	Class Type	Default User Class	USERS
Class Name	Class Type				
Default User Class	USERS				

Troubleshooting Bind and searching Issues

Whenever an unsuccessful test result is generated, to troubleshoot, it's important to understand how the search and authenticate process is initiated. The best point of reference is the GS-4 **RUN.log** file found under [\\GS4\Logs](#).

A successful Bind and Search

A search attempt first looks for the authenticated user. If successful, the LDAP Auth users Distinguish name is returned as follows:

] LDAP Auth for CN=goprintldap,CN=Users,DC=goprint,DC=com



Once authenticated an attempt is made to find the specific User entered during the test. In this case, a successful attempt was made to find the user Steve under the IT Staff OU.

**2008-11-17 16:07:28,265 DEBUG [btpool1-4:ldap.LDAPConnector]
LDAP Auth for CN=Steve,OU=IT STAFF,DC=goprint,DC=com**

Failed to find authenticated user

An error code 525 is returned when the account cannot be found. The results could be caused by a number of things:

- The authenticated user account is not located in the search path
- Authenticated username may be misspelled
- DisplayName may be required
- Incorrect search filter path
- typos exist
- Incorrect servername was provided.

] LDAP authentication for

CN=goprintldap,cn=Users,DC=goprint,DC=com failed: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data **525, vece**]

Wrong password provided by authenticated user

Incorrect passwords are represented by a 52e error

LDAP authentication for CN=goprintldap,CN=Users,DC=goprint,DC=com failed: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, **data 52e, vece**]

525 - user not found

52e - invalid credentials

Authenticated user and end-user accounts are found but invalid password was entered by the end-user. Note the 52e error below

LDAP Auth for CN=goprintldap,CN=Users,DC=goprint,DC=com

User account Fred is found but an error 52e is returned, representing invalid credentials were entered.



2008-11-20 01:00:43,609 INFO [btpool1-3:ldap.LDAPConnector] LDAP authentication for CN=fred,CN=Users,DC=goprint,DC=com failed: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, **data 52e**, vece]

End user account does not exist

LDAP Auth for CN=goprintldap,CN=Users,DC=goprint,DC=com

2008-11-20 01:23:06,562 DEBUG [btpool1-3:authentication.AuthenticationManager] Authentication failed: null

javax.naming.PartialResultException [Root exception is javax.naming.CommunicationException: goprint.com:389 [Root exception is java.net.SocketTimeoutException: connect timed

LDAP Advanced Scenario's

Multiple LDAP profiles may be created when necessary to grant different quota amounts based on a user's status such as, credit hours, undergraduate, graduate or department.




Note: GS-4 searches the top most profile first and moves downward until a match is established.

Standard Authentication

Name	Type	Active	Order
Utah Law Students	LDAP	Active	1
Utah Law Grad student quota	LDAP	Active	2
Add a Standard Authentication Connector			
Test Standard Authentication Connectors			

LDAP-Driven Accounts Using Group Membership

Authentication and assigning users to User Classes can be filter down to their group membership level. This offers greater flexibility with filtering users when they may exist in the same Organization Unit or Container.

 **Note:** the following steps pertain to managing both end-users, as well as users who can be assigned to Administrative Classes and granted various levels of system administration.

Requirements

An existing LDAP container must exist and successfully binding. For more information see the section on creating LDAP Authentication Connectors.

Accounts – Authentication Connectors:

Name	Type	Active
students	LDAP	Active

Sample: LDAP Connector

LDAP Server

Enter the LDAP server's network name.

Server Name
Security

Search Target

Set the Base DN that is the top-level target for searches.

Base DN

Search User Account


Enter the DN of a user account to use when searching the LDAP repository. Most LDAPs require an authenticated user to perform searching, and one is recommended even if not. If left blank, an 'anonymous bind' will be used to search.

Search User DN
Password



Step 1 – Select **NONE** at the LDAP Connector Attribute section

From the Default Class drop down menu select NONE

 **Important:** Setting the Default Class level to None forces the LDAP search results to look in the LDAP filters at the Class Definitions level before adding users to specific User Classes.

Account ID	sAMAccountName
Default Class	None
Class Name	
Card Number	
<input type="checkbox"/> Lookup via database query	
First Name	givenName
Last Name	sn
Reference Number	
E-Mail	mail
Attribute Browser	

Step 2 – Select LDAP Options

Navigate to Accounts – Class Definitions
Select the desired User Class and
select LDAP Options

Properties | **LDAP Options**


Class Type USER
The USER class is used to represent users. Users can be members of one or more classes. Purses are the unique combination of Class and Pay Method, and represent accounts at the transaction level for proper accounting treatments.

Select LDAP Options

Class Name Default User Class

Pay Methods	Type	Purse Name
<input checked="" type="checkbox"/>	Quota	free print funds
<input type="checkbox"/>	Allowance	Allowance

Step 3 – Enter the corresponding group membership syntax

 **Note:** Each argument must exist in its own set of parentheses. The entire LDAP statement must be encompassed in a main set of parentheses.



Scenario #1 – Single group membership

The following strings are Microsoft Active Directory examples; make the necessary adjustments for OpenLDAP.

(MemberOf=CN=students,DC=goprintcorp,DC=dyndns,DC=org)

Method 2: LDAP Filter

Membership in this Class can alternatively be driven by LDAP attributes.

Build an LDAP filter below and this Class will be automatically assigned to use match the filter.

The LDAP Filter specified here is executed in the context of the authenticated user and only those users who are present in the user's LDAP container and readable by the user are accessible.

```
(memberOf=CN=students,DC=goprintcorp,DC=dyndns,DC=org)
```

Scenario #2 – Matching Multiple Groups

& (logical AND) - **More** than one condition, and you want all conditions in the series to be true.

```
(!(memberOf=CN=med students,DC=goprintcorp,DC=dyndns,DC=org)(memberOf=CN=law students,DC=goprintcorp,DC=dyndns,DC=org))
```

The & operator states that all Arguments must be true, or match. In this case, the matching users **MUST** be a member of **BOTH** groups, ITS and staff.

```
(&(memberOf=CN=ITS,DC=goprintcorp,DC=dyndns,DC=org)  
(memberOf=CN=staff,DC=goprintcorp,DC=dyndns,DC=org))
```

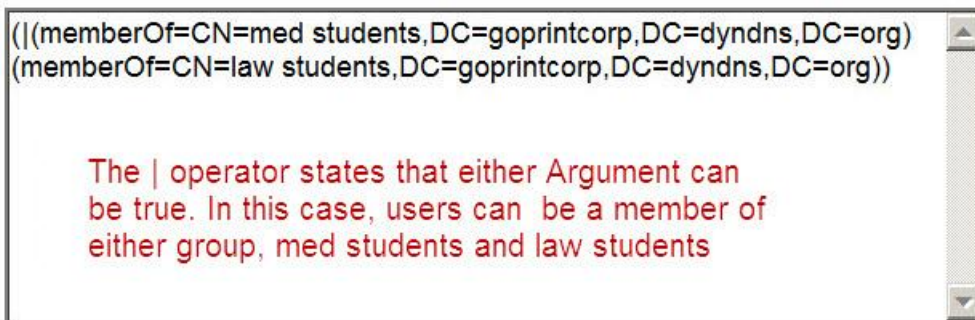
The & operator states that all Arguments must be true, or match. In this case, the matching users **MUST** be a member of **BOTH** groups, ITS and staff.

Scenario #3 – Matching Multiple Groups

| (logical or) – either condition is true

```
(|(memberOf=CN=med students,DC=goprintcorp,DC=dyndns,DC=org)(memberOf=CN=law students,DC=goprintcorp,DC=dyndns,DC=org))
```

The | Operator states that EITHER Argument can be true. In this case, users can be a member of either group med students or law students.

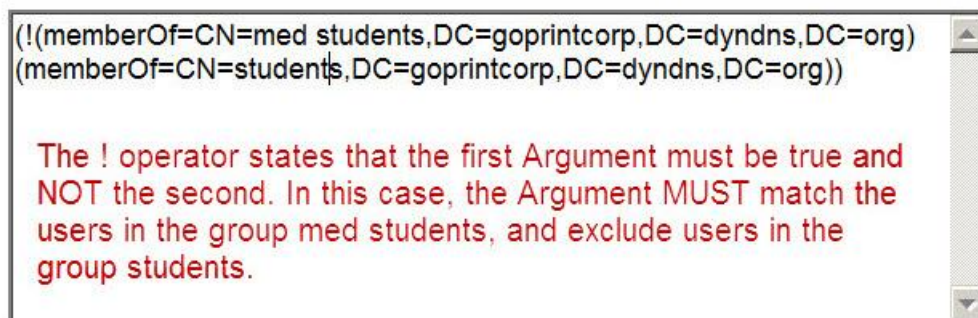


Scenario #4 – Excluding Multiple Groups

! (logical NOT) - exclude objects that have a certain attribute

```
(!(memberOf=CN=med students,DC=goprintcorp,DC=dyndns,DC=org)(memberOf=CN=law students,DC=goprintcorp,DC=dyndns,DC=org))
```

The ! Operator states that the first Argument must be true and NOT the second. In this case, the Argument MUST match the users in the group med students, and exclude users in the group students.





LDAP-Driven Accounts Using Built-in Containers

If your LDAP repository has containers for user groups, and within those containers it lists the full DN of each user who is a member of that group, then you may associate this Class to an LDAP group container. This is the easiest way to drive Class membership based on data in the LDAP repository. Simply provide the full DN of the group container that is associated with this Class of users.

Example: Microsoft provides built-in containers such as, Domain Admins, Print Operators, Users, and Administrators, plus others.

CN=Domain Admins,CN=Users,DC=goprintcorp,DC=dyndns,DC=org
CN=Print Operators,CN=Builtin,DC=goprintcorp,DC=dyndns,DC=org
CN=Users,DC=goprintcorp,DC=dyndns,DC=org

LDAP Group Membership and Print Rules

Owner Rule

Note: the user name in the Spool file has to match the user name. Reference the memberOf string under the specific path

<input type="checkbox"/>	Assume Allowed on LDAP Failure
Source of Groups	LDAP: Grad student quota
Group Names	(&(memberOf=cn=library,OU=Library,DC=goprin

String MUST contain reference to: (cn=\${User}))

Example:

(&(memberOf=cn=library,OU=Library,DC=goprint,DC=com)(cn=\${User}))

Make sure to assign the Owner Rule to the Base Pricing Section of the Price Sheet!